



Maine State Government
Dept. of Administrative & Financial Services
Office of Information Technology (OIT)

Mobile Device Policy

I. Statement

All *mobile devices*¹ that connect to the *State network*², must comply with this policy, regardless of whether they are personal (*BYOD*)³ or State-issued devices.

II. Purpose

The purpose of this Policy is to provide criteria for *mobile device* access to the *State network* in a manner that protects the confidentiality, availability, and integrity of *State information assets*.⁴

III. Applicability

This policy describes acceptable methods for a *mobile device* to connect to the *State network*. It is agnostic of the individual technology or protocol used to make the connection, and provides guidelines that cover all *mobile devices* and methods of connection. Policy scope is limited to consumer-grade computing and communication devices (smartphones, tablets, etc.) that run a mobile operating system.

This policy applies to all *mobile devices*. Registration with OIT is required for any personal (*BYOD*) or State-owned *mobile device* that connects to the *State network*. Registration is per user/per device.

IV. Responsibilities

A. Agency Management:

1. Approve requests to acquire and connect State-owned *mobile devices* to the *State network*.
2. Approve requests to connect personal (*BYOD*) *mobile devices* to the *State network*.
3. Approve Mobile Device Management support costs for State-owned and personal (*BYOD*) mobile devices that are authorized by the agency for business use.

¹ See Definition [C]

² See Definition [G]

³ See Definition [A]

⁴ See Definition [E]

Mobile Device Policy

4. Notify OIT Customer Support as soon as possible regarding any transition (transfers, terminations, etc.) of any *mobile device* holders.
5. Collect back any State-owned *mobile device* once it is no longer required (transfers, terminations, etc.).
6. Provide reimbursements (if applicable) toward official use of personal (*BYOD*) *mobile devices*.

B. User (*Mobile Device* Holder):

1. Protect the *mobile device* from theft, damage, abuse, and unauthorized use.
2. Ensure that a separate *corporate container*⁵ is setup for any personal (*BYOD*) *mobile device* and that any access to the *State network* takes place only through the *corporate container*. No data may traverse between the *corporate container* and the personal side of a (*BYOD*) *mobile device*.
3. Ensure that they remain the only user of the *corporate container* of any *mobile device* that they use to connect to the *State network*.
4. Provide *Mobile Device* Acknowledgement (attesting they understand acceptable usage, Freedom of Access Act requirements, Personal Data Act risks, security of State data, right for OIT to wipe the *mobile device* for security issues, limited OIT support for *mobile devices*, etc.) for any *mobile device* that they use to connect to the *State network*.
5. Ensure no modifications occur to either the *mobile device* or its operating system that could potentially violate or void the manufacturer's warranty or alter the manufacturer's standard security configuration. This includes, but is not limited to "jail breaking" an iOS device or "rooting" an Android device.
6. Immediately notify OIT Customer Support 207-624-7700 of any lost, misplaced, or stolen *mobile device* with *State network* access.

C. Office of Information Technology:

1. Register and manage State-owned and personal (*BYOD*) *mobile devices* that connect to the *State network*.
2. Assist users with *mobile device* configuration so that they can access the *State network*. OIT's troubleshooting assistance can only be on a best-effort basis, since OIT does not maintain *mobile devices*. Users will have to coordinate assistance from OIT and the wireless carrier, if applicable. The only OIT deliverable is access to the

⁵ See Definition [B]

Mobile Device Policy

State network.

3. Utilize *Mobile Device Management (MDM)*⁶ software for to all *mobile devices* connecting to the *State network*. This includes installing client MDM software to each *mobile device*.
4. Wipe (format) or lock the *mobile device* in the event of a security issue. This includes, but is not limited to; wiping the *corporate container* for lost/misplaced/stolen devices and locking devices exceeding the maximum number of consecutive unsuccessful device login attempts.

V. Directives

- A. *Mobile device* operating systems supported include currently supported versions (by the original equipment manufacturer) of Google Android, Apple iOS, Windows Phone, and Blackberry.
- B. *Mobile devices must* have passwords. For personal *BYOD mobile devices*, the password for the *corporate container* must be at least eight characters in length, with at least one uppercase alpha, one lowercase, alpha and one numeric character. A non-expiring password is acceptable. The pure phone feature will always remain unlocked.
- C. *Mobile devices must* lock after a maximum of 15 minutes of inactivity. Password is required to unlock.
- D. After ten (10) consecutive unsuccessful login attempts, the *mobile device* will automatically be locked. For personal (*BYOD*) *mobile devices*, automatic locking is of the *corporate container* only, not the entire device.
- E. *Mobile devices* reported as lost, misplaced, or stolen *must* be wiped (formatted). For personal (*BYOD*) *mobile devices*, automatic wiping is of the *corporate container* only, not the entire device. Users are strongly encouraged to back up the contents of their personal (*BYOD*) *mobile device*. Upon request, OIT may consent to wiping personal data.
- F. All relevant State, Agency, and DAFS-OIT policies, including [FOAA for State contents \(Title 1, Chapter 13\)](#)⁷ and the [Notice of Risk to Personal Data Act \(Title 10, Chapter 210-B\)](#)⁸, apply to the *corporate container* of *mobile devices*, irrespective of whether such access is effected via a State-owned or a personal (*BYOD*) *mobile device*.
- G. All State, Agency, and/or DAFS-OIT Acceptable Usage Policies apply while connected to the *State network*, irrespective of whether such access is via a State-owned or a personal (*BYOD*) *mobile device*. Consequently, even when the *State network* access is via a personal (*BYOD*) *mobile device*, the H.R. Directors and the Assistant Attorneys General may initiate forensic audits on the *corporate container* of such devices. It is not OIT's intent to conduct forensic

⁶ See Definition [D]

⁷ <http://www.mainelegislature.org/legis/statutes/1/title1ch13sec0.html>

⁸ <http://www.mainelegislature.org/legis/statutes/10/title10ch210-bsec0.html>

Mobile Device Policy

investigation on the personal container. Additionally, while connected to the *State network*, applications not relevant to State business may be quarantined so they cannot operate.

H. Should the *mobile device* store, even temporarily, *Personally Identifiable Information (PII)*⁹ or any other high-risk data, the device must be encrypted to the AES-256 strength.

I. The agency and/or the *mobile device* holder are responsible for provisioning all client-side product licenses in the corporate container.

J. For the purpose of access audit to state I.T. assets, the *corporate container* of each device *must* have one, and only one, designated user. All *mobile device* holders *must* vouch that they do not share the *corporate container* of their device with any other person (including family members) as a condition of using the device to access State resources.

K. Since OIT does not maintain *mobile devices*, OIT's troubleshooting assistance can only be on a best-effort basis. Users will have to coordinate assistance from OIT and the wireless carrier, if applicable. The only OIT deliverable is access to the *State network*.

L. Should statutory restrictions forbid particular agency stakeholders from accessing specific state information assets from non-state devices, then this policy does *not* change that.

M. The State is held harmless for any damage resulting from a personal *mobile device* being used for State business, having MDM software installed, and/or accessing the *State network*.

N. Failure to comply with any of the above provisos may lead to termination of access to the *State network*.

VI. Definitions

A. BYOD: Bring Your Own Device, permitting employees to use personally owned mobile devices in the workplace and to use those devices to access resources (calendar, e-mail, file services, applications, etc.) in the *State network*.

B. Corporate Container: The compartment of a *mobile device* designated specifically for work purposes. For State-owned *mobile devices*, this is the entire device. For personal (*BYOD*) *mobile devices*, this is a separate container setup on the device for work use, distinct from the container for personal use.

C. Mobile Devices: Computing and/or communication devices, running a mobile operating system (such as Google Android, Apple iOS, Microsoft Windows Phone, BlackBerry OS, etc.), as opposed to desktop-class operating system (such as Windows, Mac OS, Ubuntu, etc.).

D. Mobile Device Management (MDM): is the software that provides the following functions; software distribution, policy management, inventory management, security management, and

⁹ See Definition [F]

Mobile Device Policy

service management for devices running a mobile operating system.

- E. Information Assets: Business applications, system software, development tools, utilities, etc.
- F. Personally Identifiable Information (PII): Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Refer to [Maine Public Law 10 MRSA § 1347](#)¹⁰ for a more detailed definition. PII includes, but is not limited to Protected Health Information (PHI), Federal Tax Information (FTI), and Federal Education Rights and Privacy Act (FERPA) Information.
- G. State network: The State of Maine Wide Area Network, State of Maine Demilitarized Zone (DMZ) networks, or any other secure network managed by the State of Maine.

VII. References

VIII. Document Information

This policy is a direct successor to the *Non-OIT Managed Mobile Device Policy*. It also replaces the *Standard for the Use of Blackberry Mobile Devices*.

Initial Issue Date: July 31, 2013

Latest Revision Date: February 9, 2015

Point of Contact: Henry Quintal, Architecture-Policy Administrator, OIT, 207-624-8836.

Approved By: James R. Smith, Chief Information Officer, OIT, 207-624-7568.

Position Title(s) or Agency Responsible for Enforcement: Greg McNeal, Chief Technology Officer, OIT, 207-624-7568.

Legal Citation: 5 M.R.S.A. Chapter 163 Section 1973 paragraphs (1) B and (1) D, which read in part, “The Chief Information Officer shall:” “Set policies and standards for the implementation and use of information and telecommunications technologies...” and “Identify and implement information technology best business practices and project management.”

Waiver Process: See the [Waiver Policy](#)¹¹.

¹⁰ <http://www.mainelegislature.org/legis/statutes/10/title10sec1347-A.html>

¹¹ <http://maine.gov/oit/policies/waiver.htm>